

Standard Operating Procedure

Information Technology Security Plan Template, Requirements, Guidance and Examples

ITS-SOP-0016C

Version Date: 20080401

Effective Date: 20080417

Expiration Date: 20110417

Responsible Office: Office of the Chief Information Officer

Document Change and Review History

Version Number	Summary of Changes	Changes Made/Reviewed By	Date
1.0	Initial Release		10/5/05
2.0	Updated for NIST 800-18 Rev. 1	Sotiris Baxevanis	3/24/06
2.1	Updated per OCIO comments	Sotiris Baxevanis	5/4/06
2.2	Updates for consistency with Master SSPs (ITS-SOP-0032) and FIPS 199 categorization procedure (ITS-SOP-0019B)	Andy Boncek/ Marion Meissner	7/11/06
3.0	Updated during RMS Transition to 4.5 to adjust SSP template, checkbox structure, and remove master/subordinate language	D. Kniffin/A. Keim	3/4/08
3.1	Updated to reflect RMS Transition Team and OCIO comments	D. Kniffin/A. Keim	3/25/08
3.2	Edit for structure and formatting	T. Fryer	4/1/08

TABLE OF CONTENTS

1. PURPOSE	1
2. SCOPE	1
3. APPLICABLE DOCUMENTS	1
4. ROLES AND RESPONSIBILITIES	1
5. PROCESS	2
6. APPROVAL	2
APPENDIX A: GLOSSARY	3
APPENDIX B: SSP TEMPLATE	4

1. Purpose

This document defines the information technology (IT) system security plan (SSP) template and provides requirements, guidance and examples for the completion of these plans. The information captured in the SSP template is critical for the certification and accreditation (C&A) of the system and the granting of an authorization to operate that system. The template acts as an outline to capture information regarding the system's function, operational concept, the type and category of information processed or stored on the system, risk assessment results, and the implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls.

The SSP template defined in this standard operating procedure (SOP) is based on Federal Information Processing Standard (FIPS) 199, FIPS 200, NIST SP 800-18 Rev. 1 and other NIST 800 series guidance. Additionally, ITS-SOP-0030 and ITS-SOP-0031 define the procedures for the C&A of NASA IT systems. ITS-SOP-0007 details the numbering schema for NASA system security plans, and ITS-SOP-0019B describes the process to define information categories of NASA IT systems.

2. Scope

This SOP applies to all personnel who are responsible for or involved in preparing SSP documentation for NASA information systems.

3. Applicable Documents

- a. NPD 2810.1C "NASA Information Security Policy"
- b. NPR 2810.1A "Security of Information Technology"
- c. NIST SP 800-18 Rev. 1 "Guide for Developing Security Plans for Federal Information Systems"
- d. NIST SP 800-30 "Risk Management Guide for Information Technology Systems"
- e. NIST SP 800-37 "Guide for Security Certification and Accreditation of Federal Information Systems"
- f. NIST SP 800-53 "Recommended Security Controls for Federal Information Systems"
- g. NIST SP 800-53A "Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems"
- h. NIST SP 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories"
- i. FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems"
- j. FIPS 199 "Standards for Security Categorization of Federal Information and Information Systems"
- k. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*
- l. Federal Information Security Management Act of 2002 (FISMA)

4. Roles and Responsibilities

The following roles and responsibilities are applicable to this SOP:

Information System Owner (ISO)

- a. Responsible for the development of SSPs in accordance with this SOP

Security Documentation Creator/Preparer

- a. Ensures that the SSP is developed in accordance with this SOP, entered into the IT Security documentation repository appropriately and updated as necessary

NASA Senior Agency Information Security Officer (SAISO)

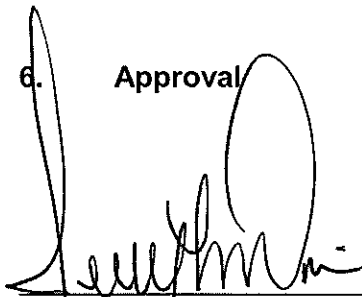
- a. Responsible for updating this SOP to address published updates by NIST as well NASA policy requirements

5. Process

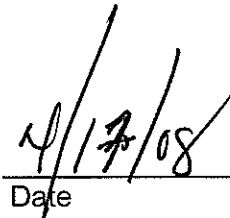
Appendix B of this SOP provides a complete SSP template including cover pages and appendices and contains instructions and examples. This template is the definitive source of the security plan template for systems in NASA's IT Security Risk Management System (RMS). All NASA SSPs shall be completed online using RMS, but this SOP shall serve as the standard template definition for RMS SSPs. In order to assist the plan writer, the template contains the following sections:

- a. Template – Any section of the template not included within brackets is mandatory and requires that the writer complete the information for the section or utilize the language provided; complete the defined table, address specific questions, etc.
- b. [INFORMATION to be filled in] – Text in brackets must be replaced by the appropriate information specific to the plan.
- c. *{Instructions: specific instruction text}* – Any section in italics and braces provides specific requirements, guidance, and examples for each plan section to ensure completeness and consistency among security plans. These instructions should be deleted from the final SSP.

6. Approval



Jerry L. Davis
Deputy CIO IT Security
Senior Agency Information Security Officer


Date

Appendix A: Glossary

Acronym	Term	Explanation
ISO	Information System Owner	A NASA official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals.
IT	Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.
SAISO	Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
SSP	System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Appendix B: SSP Template

[SYSTEM NAME] ([SYSTEM ABBREVIATION])

System Security Plan (SSP)

Prepared for:
[AGENCY]
[ADDRESS]

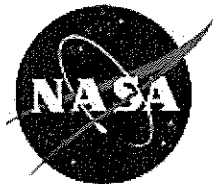
[VERSION NUMBER]

[DATE]

Issue Date: *[MM-DD-YYYY]*

THE ATTACHED MATERIALS CONTAIN [AGENCY] INFORMATION THAT IS "FOR OFFICIAL USE ONLY", OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS MUST BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH [AGENCY] MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND, WHEN UNATTENDED, MUST BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.



National Aeronautics and
Space Administration

REVIEW AND APPROVAL SIGNATURES

This System Security Plan for the [SYSTEM NAME] was prepared for the exclusive use of the [AGENCY].

Reviewed by: _____
Information System Owner Date

I have reviewed and concur with the contents of this plan.

Approved by: _____
Sr. Agency Information Security Officer Date

Approved by: _____
Authorizing Official Date

DOCUMENT CHANGE HISTORY

C&A Phase	Version	Date	Change POC	Approved By	Change Description

TABLE OF CONTENTS

REVIEW AND APPROVAL SIGNATURES

DOCUMENT CHANGE HISTORY

1.0 SYSTEM NAME & TITLE

2.0 INFORMATION SYSTEM CATEGORIZATION

2.1 Information Types

2.2 Security Categorization

3.0 INFORMATION SYSTEM OWNER

4.0 AUTHORIZING OFFICIAL

5.0 OTHER DESIGNATED CONTACTS

6.0 ASSIGNMENT OF SECURITY RESPONSIBILITY

7.0 SYSTEM OPERATIONAL STATUS

8.0 INFORMATION SYSTEM TYPE

9.0 SYSTEM DESCRIPTION

9.1 Purpose

9.2 Function

10.0 SYSTEM ENVIRONMENT

10.1 Hardware

10.2 Software

10.3 Network Configuration

10.4 Accreditation Boundary

11.0 SYSTEM INTERCONNECTION/INFORMATION SHARING

12.0 RELATED LAWS/REGULATIONS/POLICIES

13.0 MINIMUM SECURITY CONTROLS

13.1 Scope

13.1.1 Control Descriptions

13.1.2 Minimum Assurance Requirements

13.2 Management Controls

13.2.1 Certification, Accreditation, and Security Assessments

13.2.2 Risk Assessment

13.2.3 Planning

13.2.4 System and Services Acquisition

13.3 Operational Controls

13.3.1 Physical and Environmental Protection

13.3.2 Personnel Security

13.3.3 Media Protection

13.3.4 Configuration Management

13.3.5 Contingency Planning

13.3.6 Incident Response

13.3.7 Awareness and Training

13.3.8 Maintenance

13.3.9 System and Information Integrity

13.4 Technical Controls

13.4.1 Access Control

13.4.2 Identification and Authentication

13.4.3 Audit and Accountability

13.4.4 System and Communications Protection

14.0 PLAN COMPLETION

15.0 PLAN APPROVAL AND EFFECTIVE DATE

1.0 SYSTEM NAME AND TITLE

System Name: [SYSTEM NAME]

System Abbreviation: [SYSTEM ABBREVIATION]

FISMA Identification: [FISMA ID]

2.0 INFORMATION SYSTEM CATEGORIZATION

{Instructions: The system owner shall use the process described in ITS-SOP-0019 to determine the information types processed or stored by the system. In the case where the system is a collection of explicitly defined applications, those applications shall first be categorized and then the high water mark of these applications will determine the information system categorization.}

2.1 INFORMATION TYPES

{Instruction Note: NF-1746 and NF-1748 can be used to document the Information Security Categorization and information types, justify variances, and obtain electronic signature approvals.}

The following tables identify the information types that are input, stored, processed, and/or output from [SYSTEM ABBREVIATION]. The selection of the information types is based on guidance provided by NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, OMB Federal Enterprise Architecture Program Management Office Business Reference Model 2.0, and FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*.

The tables also identify the security impact levels for confidentiality, integrity, and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity, and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

In any instances where the owner has chosen to deviate from the NIST recommended impact level, complete justification has been provided.

INFORMATION TYPE (Derived from NIST SP 800-60)		
INFORMATION SUB-TYPE		
Confidentiality Impact Level	NIST:	OWNER:
Integrity Impact Level	NIST:	OWNER:
Availability Impact Level	NIST:	OWNER:
Justification for any deviation from the NIST recommended impact level		

EXAMPLE (complete one table for each category of data stored or used by the system):

INFORMATION TYPE (Derived from NIST SP 800-60)	C.2.1.1 Corrective Action Information (pg. 22)
--	---

INFORMATION SUB-TYPE		
Confidentiality Impact Level	NIST: low	OWNER: low
Integrity Impact Level	NIST: low	OWNER: low
Availability Impact Level	NIST: low	OWNER: low
Justification for any deviation from the NIST recommended impact level		

INFORMATION TYPE (Derived from NIST SP 800-60)	C.2.3.6 Workforce Planning Information (pg. 38)	
INFORMATION SUB-TYPE		
Confidentiality Impact Level	NIST: low	OWNER: low
Integrity Impact Level	NIST: low	OWNER: low
Availability Impact Level	NIST: low	OWNER: low
Justification for any deviation from the NIST recommended impact level		

2.2 Security Categorization

Based on the information provided in section 2.1, the security impact levels for each of the three security objectives of confidentiality, integrity, and availability are identified below.

Security Objective	Security Impact Level (L/M/H)
Confidentiality:	
Integrity:	
Availability:	

Table: Security Impact

Based on the information provided in the Security Impact table above, the required protection level for [SYSTEM ABBREVIATION] has been identified and is reflected in the following High Water Mark table. The high water mark represents the minimum level of security controls appropriate for [SYSTEM ABBREVIATION].

[SYSTEM ABBREVIATION] High Water Mark	[HIGH/MODERATE/LOW]
--	----------------------------

Table: High Water Mark

3.0 Information System Owner

The following individual is designated as the system owner. This designated person has sufficient knowledge of the system to provide additional information or points of contact as needed.

{Instruction Note: the person specified is the key point of contact (POC) for this information system and is responsible for coordinating system development life cycle (SDLC) activities

specific to this information system. The system owner also has expert knowledge of the system capabilities and functionality.}

Name:
Title:
Organization:
Address:
Phone:
E-Mail:

4.0 Authorizing Official

The following individual is designated as the Authorizing Official.

{Instruction Note: This designated person is the senior management official who has the authority to authorize the operation (accredit) of this information system and accept any residual risk(s) associated with this information system.}

Name:
Title:
Organization:
Address:
Phone:
E-Mail:

5.0 Other Designated Contacts

The following individual had been assigned security responsibility for this system. This assignment has been officially designated in writing.

{Instruction Note: the named individual has been assigned key responsibilities for/within this information system and can therefore address inquiries regarding system characteristics and operation.}

Name:
Title:
Organization:
Address:
Phone:
E-Mail:

6.0 Assignment of Security Responsibility

The following individual has been assigned security responsibility for this system. This assignment has been officially designated in writing.

{Instruction Note: If multiple individuals have been assigned the security responsibilities within a system, simply repeat the table below as needed and differentiate each person's security role.}

Name:
Title:

Organization:

Address:

Phone:

E-Mail:

7.0 System Operational Status

The system is in the following life cycle status:

- ☐ Operational - the system is operating.
- ☐ Under development - the system is being designed, developed or implemented.
- ☐ Undergoing a major modification - the system is undergoing a major conversion or transition.

8.0 Information System Type

This system has been classified as the following information system type:

☐ General Support System - An interconnected set of information resources under the same direct management control that shares common functionality.

☐ Major Application - an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

[SYSTEM ABBREVIATION] has been categorized as an **Industrial Control System**, and therefore the additional controls, enhancements, and supplemental guidance in NIST SP 800-53, Appendix I are applicable to the system.

9.0 SYSTEM DESCRIPTION

9.1 Purpose

{Instructions: Describe the general purpose of the system. For example,

The [SYSTEM ABBREVIATION] provides a means of data transport for users assigned to [AGENCY]. The [SYSTEM ABBREVIATION] provides unclassified but sensitive network services including e-mail, web browsing, office automation, and connectivity for specialized computer applications. In this section, present a brief description (one-three paragraphs) of the purpose of the system (e.g., economic indicator, network support for an organization, business census data analysis, crop reporting support). Describe how the system relates to or supports the intended mission.}

9.2 Function

{Instructions: Describe the general functionality of the system. For example,

[SYSTEM NAME] encompasses a variety of engineering and administrative applications, some on single-use platforms. It is currently running on Microsoft Windows 2000. Each [DIVISION] uses this integrated administrative information system."

[SYSTEM NAME] is structured so that it can be customized in certain specialized areas, and most local centers have taken advantage of this flexibility. Applications within [SYSTEM NAME]

support numerous areas, including baggage imaging, supply management, decision support, transportation research, and education.

Note: If a major application is hosted on the system, this plan should reference the major application's system security plan.

10.0 System Environment

{Instructions: Describe the environment where the system is housed. For example,

The [SYSTEM ABBREVIATION] is a general purpose, multi-user system used throughout the [AGENCY]. It provides a myriad of electronic services (such as electronic mail, word processing, spreadsheets, electronic forms, databases, etc.) and provides a gateway to the Internet. More importantly, the [SYSTEM ABBREVIATION] provides the staff with the tools to improve business processes. The result is increased efficiency and effectiveness.

Access to the system is via workstations operating on Windows-family Operating Systems (O/S) including Windows NT 4.0, Windows 2000 Professional, and Windows XP, "thin" client terminals, and various models of "dumb" terminals. Microsoft Windows client workstations connect to [SYSTEM ABBREVIATION] over a Windows network using terminal emulation software and the Remote Procedure Call (RPC) Broker. There is access from the Intranet to both the wide area network (WAN) and to the Internet via the Internet Gateways. [AGENCY]-approved firewalls are positioned between the Intranet and the Internet Gateways. DEC VT and other types of terminals connect to [SYSTEM ABBREVIATION] via Ethernet and terminal servers. There is limited dial-in access to [SYSTEM ABBREVIATION] via a Remote Access Server (RAS), which resides inside the computer room and uses Windows authentication to the network. This access via RAS is being phased out. Access via RAS is in use by IS staff members and other authorized users. This system has replaced a modem bank and provides a secure remote access capability.

10.1 Hardware

{Instructions: Describe the primary hardware utilized by the system. For example,

The [SYSTEM ABBREVIATION] consists of servers, switching devices, and other network components required to provide network users with access to application servers, data storage facilities, file transfer capabilities, and external data communications. The Primary Domain Controller (PDC) and parent Exchange e-mail server for the [SYSTEM ABBREVIATION] are located at [LOCATION]. Primary/Backup Domain Controllers and Exchange Servers are located at 15 remote locations throughout the region. There are 36 other remote Project/Resident Office locations with only workstations or PCs connected to the network via leased frame relay lines.

The Computer Room, located at [LOCATION], is the point of presence (PoP) for the frame relay network that connects the [SYSTEM ABBREVIATION] to the [NETWORK NAME] through a [SIZE] frame connection. The T1 trunk from the network terminates in a single [EQUIPMENT] maintained by [MANUFACTURER]. The CSU/DSU passes data over a V.35 interface to a Cisco 3600 series router for region edge routing.

Hardware	Model Number	Serial Number	Location	Quantity
Cabletron 6000 Ethernet Switch 2	C292	212349	Bldg 4000 Room 32	5

Hardware

}

10.2 Software

{Instructions: Describe the primary software utilized by the system. For example,

The majority of the [SYSTEM ABBREVIATION] servers are configured with Microsoft Windows 2003 SP1. Five servers are configured with Sun Solaris Version 8, two with Sun Solaris Version 2.7, one with Sun Solaris Version 2.6, two with Novell Version 5.1, and two with SCO UNIX Version 5.05. [SYSTEM ABBREVIATION] users access network services via a mixture of Windows NT 4.0 workstations and Windows 2000 Professional workstations.

One Microsoft Windows NT Server is configured as the Microsoft Exchange server, running Exchange 5.5 with Service Pack 4. One server is loaded with Intrusion Detection System (IDS) software, and one is loaded with Surf Control application software that monitors user community Internet/Intranet use. The remaining Windows NT servers are configured to support Windows Internet Naming Service (WINS), Network File Storage, and Network Printing.

Location	Operating System/ Application Software	Use

Software

}

10.3 Network Configuration

{Instructions: Describe network parameters and configuration utilized by the system, along with physical and logical diagrams as appropriate for ease in depiction..

External data flow into and out of the [SYSTEM ABBREVIATION] is through the [AGENCY] Network. Connectivity to the [AGENCY] network is through a T1 frame connection at the [NETWORK OPERATIONS CENTER] that terminates in a single ADC Kentrox Data Smart 656 CSU/DSU. The CSU/DSU passes data over a V.35 interface to a Cisco 3600 series router for District edge routing.

The [SYSTEM ABBREVIATION] within the [LOCATION] is a mix of Ethernet 10/100Base-T/FOIRL segments. Each Cabletron 6000 switch and hub in the [LOCATION] Building is connected to the main Cabletron 9000 switch via Ethernet 100Base-FOIRL segments. Connectivity between the [SYSTEM ABBREVIATION] and the remote offices is accomplished through a 3Com NETBuilder II router connected to frame relay leased fractional T1 lines. Three point-to-point T1 lines are also used to connect each of the three offices at the remote site.

The [SYSTEM ABBREVIATION] uses ports, protocols and services identified in the following table.

Ports	Protocols	Service	Direction
22	SSH	Secure Shell	Bi-directional

Ports, Protocols, and Services allowed through the Firewall.

}

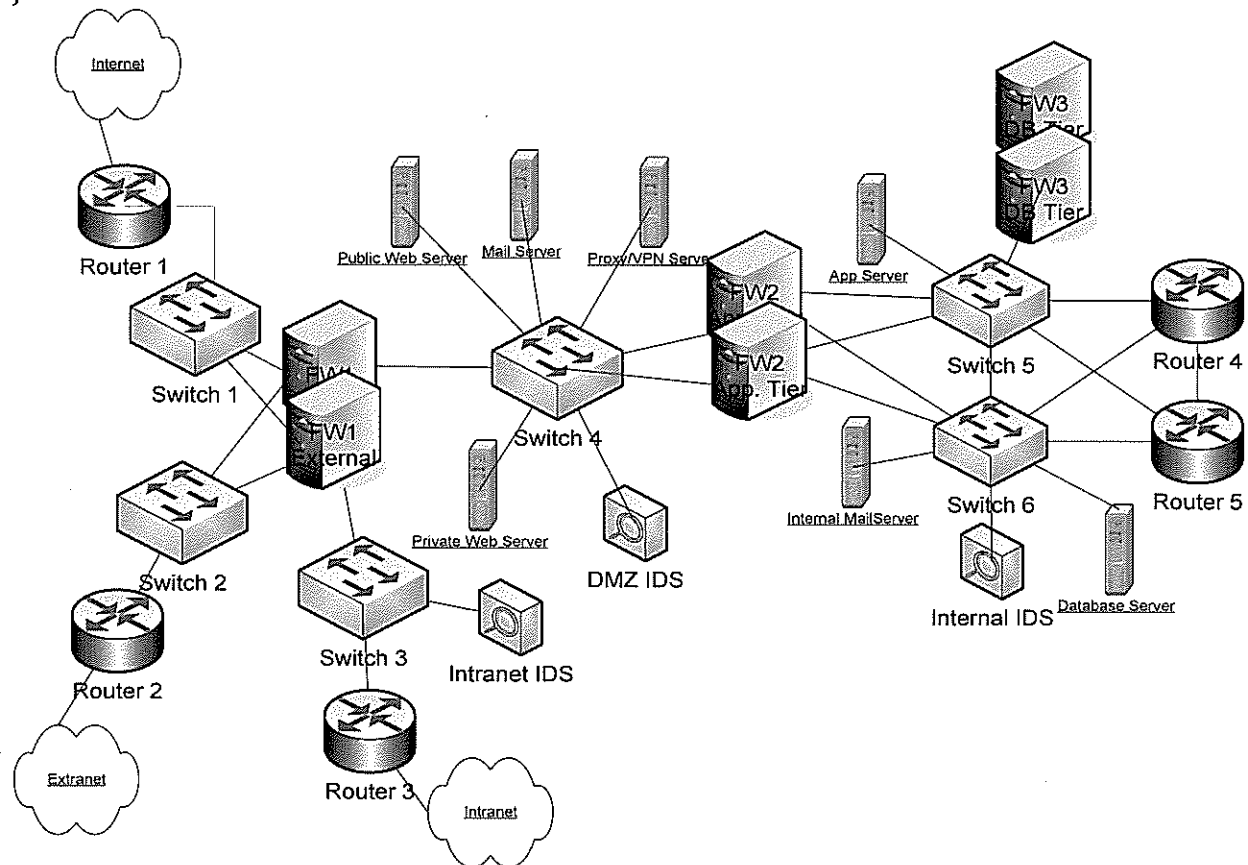
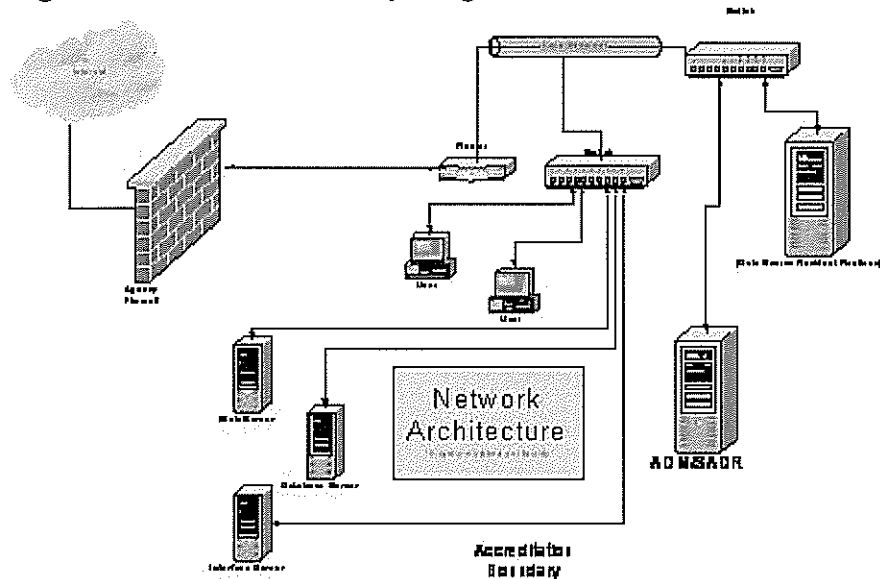


Figure 1 Physical Diagram

Fig: Accreditation Boundary Diagram



11 System Interconnections/Information Sharing

{Instructions: Describe and/or list any interconnections with other systems and ensure that appropriate Interconnect Service Agreements (ISA)/MOUs/MOAs are in place if necessary. All interconnections with systems outside your accreditation boundary must be listed in the table below. For example,

The following table contains relevant information about systems connected to the [SYSTEM ABBREVIATION].

System ID/Name	Org.	Type	Agreement	Date	FIPS 199 Category	C&A Status	Auth. Official

System Interconnections

Table: Service Level Agreements with other Systems

Instruction Note: CA-3 requires the organization to formally authorize all connections from the information system to other information systems with different security requirements outside of the accreditation boundary through the use of system connection agreements. NIST Special Publication 800-47 provides guidance on connecting information systems.}

12 Related Laws/Regulations/Policies

{Instructions: List the laws and regulations that govern your IT system. For example,

The following are laws, regulations and policies that affect the system.

5 U. S. C. 552, Freedom of Information Act, 1967

5 U. S. C. 552a, Privacy Act, 1974

FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems

NIST SP 800-30, Risk Management Guide for Information Technology Systems

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems

NIST SP 800-42, Guideline on Network Security Testing

NIST SP 800-53, Recommended Security Controls for Federal Information Systems

NIST SP 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories

NIST SP 800-61, Computer Security Incident Handling Guide

NIST SP 800-64, Security Considerations in the Information System Development Life Cycle

OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems

Public Law (PL) 99-474, The Computer Fraud and Abuse Act of 1986

PL 93-502 - Freedom of Information Act 1974

Presidential Decision Directive (PDD-63), Critical Infrastructure Protection

Federal Information Security Management Act of 2002 (FISMA)

}

13 Minimum Security Controls

13.1 Scope

{Instructions: Per NPR 2810.1A, a NASA system inherits all requirements and tailoring of NIST SP 800-53 controls from the Agency controls, as issued by the NASA Office of the CIO, and from all applicable common control packages.}

SSPs created natively in RMS will be populated with the Agency controls and all applicable common controls.}

The following sections (13.2, 13.3, and 13.4) contain the management, operational, and technical controls that have been selected for the [SYSTEM NAME]. The controls were taken from NIST SP 800-53 and are based on the system's security categorization per FIPS 199.

13.1.1 Control Descriptions

Each control section provides a thorough description of how the security is being implemented or planned to be implemented. The descriptions contain: 1) the security control title; 2) indicates if the security control is a common control and who is responsible for its implementation; 3) whether the control is applicable or acceptable for the system; 4) a statement of the control with any applicable enhancements; and 5) a description of how the control is being implemented or planned to be implemented and any tailoring/scoping considerations.

[Control #] [Control Name]

This control is:

[] Common Control.

Implemented by:

POC:

[] Not Applicable.

[] Not Accepted.

[] Accepted. If accepted, you must indicate your choice for continuous monitoring.

[] Selected for annual review.

[] Selected for review in year:

(Note: if Not Applicable or Not Accepted, provide justification below in Implementation Detail)

Control:

Implementation Detail:

{Instructions: EVERY control in the appropriate baseline annex from NIST SP 800-53 must be addressed in this SSP, whether it is a common control, or not applicable to/not accepted by this system. For each control, use the entire control template and fill out the appropriate sections. NOTE: SSPs created in RMS will be populated with the Agency controls and all applicable common controls (if they exist natively within RMS). SSPs created manually must incorporate the current version of the Agency controls, as issued by the NASA Office of the CIO, and the common controls from the applicable packages.}

NOTE: RMS will provide an area for Supplemental Guidance and Enhancement Supplemental Guidance, however this information will remain only in RMS and will not appear in the printed, completed security plan.

[Control #] [Control Name]

{Instructions: Use the baseline control requirements from NIST SP 800-53, annex 1, 2 or 3, as appropriate for the system's FIPS 199 security category.}

This control is:

[] Common Control.

(see Control)

{Instructions: This indicates that the control is implemented by the Security Plan and has been verified as meeting the NIST SP 800-53 requirements. If a control is "Common", it can apply to organizational information systems, a group of systems at a specific site or information systems, subsystems or applications (i.e. common hardware, software and/or firmware) at multiple operational sites. Common controls are implemented based on recommendations and/or requirements of NIST, FISMA, FIPS, NASA Agency, Contractor, Mission or equivalent. An example of this would be PL-01, where the security planning policies and procedures are defined and published by the Agency to satisfy this control. NASA Agency controls are inherited in the standard RMS Security Plan template. It is recommended that this option be used.}

Implemented by:

{Instructions: Indicate the system, organization, or package name the common control is inherited from.}

POC:

{Instructions: Indicate the office or individual responsible for the development, implementation, and assessment of the control..}

[] Not Applicable to this System. (see Implementation Detail for justification)

{Instructions: There may be controls that are not applicable to a particular network or system. For instance, a control for Voice over IP is included as a baseline security control, but VoIP might not be implemented on the system. In that case the control would be considered Not Applicable, but you must document the justification in the implementation detail section below.}

[] Not Accepted. (see Implementation Detail for justification)

{Instructions: There may be controls that are cost-prohibitive or unacceptable due to technical considerations. In that case, research should be conducted to identify an alternative, compensating control. You must fully document the reason that the control is not accepted, and state whether or not an alternative control has been implemented.}

[] Accepted. If accepted, you must indicate your choice for continuous monitoring..

{Instructions: Most controls should fall with in this category. If it is a hybrid control, both the Common Control box AND the Accepted box will be checked by the common package that initially answered a portion of the control and inherited within the template. Once a control is accepted, indicate whether the control has been selected for annual review or not. Select only ONE option below.}

[] Selected for annual review.

{Instructions: This indicates that the control is selected for annual review by either a requirement in the control statement, NASA policy, ,or because it is deemed critical or volatile to your system. This review can be part of the annual self-assessment by the system owner or POC and shall include verifying that the control is still applicable, reasonable, effective and functioning as intended.}

[] Selected for review in year:

{Instructions: This indicates that the control will be reviewed during the stated calendar year. This review is outside of the annual self-assessment by the system owner or POC and shall include verifying that the control is still applicable, reasonable, effective and functioning as intended This is to facilitate future planning to ensure the non-annual controls are reviewed sometime within the three(3) year cycle.}

(Note: if Not Applicable or Not Accepted, provide justification below in Implementation Detail)

Control:

{Instructions: Insert the control description from NIST SP 800-53. If the NIST 800-53 control has "organization defined parameters" such parameters should be defined by a common control package or the system owner and specified in the implementation detail section. The documentation and results of any control testing should not appear in Section 13 of the SSP, but rather in the RTM.}

Implementation Detail:

{Instructions: Description of implementation by the source organization; OR reference to POA&M for actions to be completed; OR justification for Not Applicable; OR justification for Not Accepted.}

13.1.2 Minimum Assurance Requirements

In accordance with SP 800-53, Appendix E, the focus of actions and activities put into place for each Security Control found in sections 13.2, 13.3, 13.4 of this System Security Plan, is on the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. For security controls in the high baseline, this same documentation is needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

{Instructions: Select the appropriate baseline statements from NIST 800-53 based on the information categorization of the security plan for inclusion in Section 13.1.2.}

The Low Baseline Assurance Requirement states:

“The security control is in effect and meets explicitly identified functional requirements in the control statement. Supplemental Guidance: For security controls in the low baseline, the focus is on the control being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.”

The Moderate Baseline Assurance Requirement states:

“The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions to ensure that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination. Supplemental Guidance: For security controls in the moderate baseline, the focus is on ensuring correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation to ensure the control meets its required function or purpose.”

The High Baseline Assurance Requirement states:

“The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control (including functional interfaces among control components). The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.”

Additional Requirements for Enhancing the Moderate and High Baselines:

“The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, actions to ensure that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. The control is developed in a manner that supports a high degree of confidence

that the control is complete, consistent, and correct. Supplemental Guidance: The additional high assurance requirements are intended to supplement the minimum assurance requirements for the moderate and high baselines, when appropriate, in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is required for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.”

(from NIST Special Publication 800-53, pgs. 43-44) }

13.2 MANAGEMENT CONTROLS

The Management security controls section of this SSP identifies the management safeguards and countermeasures in-place or planned for [SYSTEM NAME]. Management Controls are those safeguards and countermeasures that focus on the management of risk and the management of the information security system. They are actions that are performed primarily to support information system security management decisions.

13.2.1 Certification, Accreditation, and Security Assessments (CA)

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

(FIPS 200, Section 3, Minimum Security Requirements)

{Instructions: Example of a fully implemented Common control. No change or action by the system owner would be required.}

CA-01 Certification, Accreditation, and Security Assessment Policies and Procedures

This control is:

☒ Common Control.

Implemented by: Agency Common Controls, NASA

POC: T. Fryer, OCIO IT Security

☐ Not Applicable.

☐ Not Accepted.

☒ Accepted. If accepted, you must indicate your choice for continuous monitoring.

☒ Selected for annual review.

☐ Selected for review in year:

(Note: if Not Applicable or Not Accepted, provide justification below in Implementation Detail)

Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

Implementation Detail:

Item (i) fully satisfied by NPR 2810.1A, *Security of Information Technology*, Chapter 14 – Certification and Accreditation and OCIO Memo “Certification and Accreditation Direction for FY08” dated 11/29/07.

Item (ii) satisfied via ITS-SOP-0019B, *Procedure for the FIPS-199 Categorization of Information Systems*, ITS-SOP-0030B *C&A Process for MOD and HIGH Systems*, ITS-SOP-0031B *C&A Process for LOW Systems*, ITS-SOP-0016B *ITSP Requirements and Guidance*, ITS-SOP-0007 *System Security Plan Numbering Schema*, and ITS-SOP-0043 *Procedures for Selecting and Tailoring NIST 800-53 Common Controls*.

NASA utilizes the NASA System Security Plan Repository tools for the development, storage, and continuous monitoring of IT System Security Plans. Compliance with the above agency guidance is monitored by the Center IT Security Managers (ITSM) and Certification and Accreditation Officials (CAO). Centers are also subject to internal and external reviews of their IT Security Programs. }

13.2.2 Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

(FIPS 200, Section 3, Minimum Security Requirements)

13.2.3 Planning (PL)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

(FIPS 200, Section 3, Minimum Security Requirements)

13.2.4 System and Services Acquisition (SA)

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3 OPERATIONAL CONTROLS

The Operational security controls section of this SSP identifies the operational safeguards and countermeasures in-place or planned for [SYSTEM NAME]. Operational Controls are those safeguards and countermeasures that are primarily implemented and executed by people as opposed to systems and technology.

13.3.1 Physical and Environmental Protection (PE)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

(FIPS 200, Section 3, Minimum Security Requirements)

{Instructions: Example of a fully implemented Common control. No change or action by the system owner would be required.}

PE-03 Physical Access Control

This control is:

☒ Common Control.

Implemented by: Kennedy Space Center (KSC) Common Controls
POC: Lt. John Smith, KSC Security, Chief of Security

☐ Not Applicable.

☐ Not Accepted.

☒ Accepted. If accepted, you must indicate your choice for continuous monitoring.

☒ Selected for annual review.

☐ Selected for review in year:

(Note: if Not Applicable or Not Accepted, provide justification below in Implementation Detail)

Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. Control Enhancements: (1) The organization controls physical access to the information system independent of the physical access controls for the facility.

Control:

The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Implementation Detail:

This control is fully implemented. KNPR 1600.1 “KSC Security Procedural Requirements” Chapter 16, Personnel Control And Area Permits outlines procedures for review of physical access logs and key control to limited access areas. The Center Chief of Security is responsible for establishing requirements for entry to KSC and its controlled access areas/facilities, and for managing and implementing the KSC Area Permit program for controlling access to those areas/facilities. The Director, Safety and Mission Assurance is responsible for establishing safety training requirements which must be completed prior to issuance of a KSC Area Permit or TAA, authorizing unescorted access to a controlled area.

Personnel Access Control and Accountability System (PACAS) cards are uniquely coded devices used to provide automated control and accountability of personnel into and out of controlled areas through use of a card reader system. If the entry or exit is authorized, a command shall be generated to unlock the control device (turnstile, gate, or door) to permit unalarmed entry or exit. Unauthorized attempts shall initiate an alarm in the KSC Joint Communications Control Center (JCCC).

}

13.3.2 Personnel Security (PS)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.3 Media Protection (MP)

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.4 Configuration Management (CM)

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and

enforce security configuration settings for information technology products employed in organizational information systems.
(FIPS 200, Section 3, Minimum Security Requirements)

13.3.5 Contingency Planning (CP)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

(FIPS 200, Section 3, Minimum Security Requirements)

{Instructions: Example of a fully implemented control by the system owner.

This control is:

☐ Common Control.

Implemented by:

POC:

☐ Not Applicable.

☐ Not Accepted.

☒ Accepted. If accepted, you must indicate your choice for continuous monitoring.

☒ Selected for annual review.

☐ Selected for review in year:

(Note: if Not Applicable or Not Accepted, provide justification below in Implementation Detail)

Control: The organization: (i) tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions. Control Enhancements: (1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans. (2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

Implementation:

This control is fully implemented. Contingency testing is scheduled annually and was last conducted on 2/10/2008. Contingency testing was last conducted as a classroom scenario in conjunction with the annual contingency training.

}

13.3.6 Incident Response (IR)

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.7 Awareness and Training (AT)

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.8 Maintenance (MA)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

(FIPS 200, Section 3, Minimum Security Requirements)

13.3.9 System and Information Integrity (SI)

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

(FIPS 200, Section 3, Minimum Security Requirements)

13.4 TECHNICAL CONTROLS

The Technical security controls section of this SSP identifies the technical safeguards and countermeasures in-place or planned for [SYSTEM NAME]. Technical Controls are those safeguards and countermeasures that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

13.4.1 Access Control (AC)

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

(FIPS 200, Section 3, Minimum Security Requirements)

13.4.2 Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(FIPS 200, Section 3, Minimum Security Requirements)

13.4.3 Audit and Accountability (AU)

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

(FIPS 200, Section 3, Minimum Security Requirements)

13.4.4 System and Communications Protection (SC)

Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

(FIPS 200, Section 3, Minimum Security Requirements)

14.0 PLAN COMPLETION

This version of the System Security Plan was completed on _____.

15.0 PLAN APPROVAL AND EFFECTIVE DATE

The Authorizing Official's signature at the front of this System Security Plan puts this plan into effect from the date of signature.

Appendix A – Accreditation Decision Letter (Authorization to Operate)

{Instruction Note: NF-1740 can also be used to document the Accreditation Decision and provides electronic signature capability.}

From: Authorizing Official [AO]

Date:

To: Information System Owner [SO]

Subject: Security Accreditation Decision for [SYSTEM NAME]

After reviewing the results of the security certification of the [SYSTEM NAME] and its constituent system-level components (if applicable) located at [LOCATION] and the supporting evidence provided in the associated security accreditation package (including the current system security plan, the security assessment report, and the plan of action and milestones), I have determined that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is acceptable. Accordingly, I am issuing an *authorization to operate* the information system in its existing operating environment. The information system is accredited without any significant restrictions or limitations. This security accreditation is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.

The security accreditation of the information system will remain in effect as long as: (i) the required security status reports for the system are submitted to this office and to the Senior Agency Information Security officer every year; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) the system has not exceeded three years between security accreditations in accordance with Federal or Agency policy.

A copy of this letter with all supporting security certification and accreditation documentation should be retained in accordance with the Agency's record retention schedule.

Name,
Title

Date

Enclosure

Appendix B - Accreditation Decision Letter (Interim Authorization to Operate)

From: Authorizing Official
To: Information System Owner

Date:

Subject: Security Accreditation Decision for [SYSTEM NAME]

After reviewing the results of the security certification of the [SYSTEM NAME] and its constituent system-level components (if applicable) located at [LOCATION] and the supporting evidence provided in the associated security accreditation package (including the current system security plan, the security assessment report, and the plan of action and milestones), I have determined that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is *not* acceptable. However, I have also determined that there is an overarching need to place the information system into operation or continue its operation due to mission necessity. Accordingly, I am issuing an *interim authorization to operate* the information system in its existing operating environment. An interim authorization is a limited authorization to operate the information system under specific terms and conditions and acknowledges greater agency-level risk for a limited period of time. The information system is *not* considered accredited during the period of limited authorization to operate. The terms and conditions of this limited authorization are described in Attachment A.

A process must be established immediately to monitor the effectiveness of the security controls in the information system during the period of limited authorization. Monitoring activities should focus on the specific areas of concern identified during the security certification. Significant changes in the security state of the information system during the period of limited authorization should be reported immediately.

This interim authorization to operate the information system is valid for six (6) months. The limited authorization will remain in effect during that time period as long as: (i) the required security status reports for the system are submitted to this office and to the Senior Agency Information Security Officer every three (3) months; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) continued progress is being made in reducing or eliminating vulnerabilities in the information system in accordance with the plan of action and milestones. At the end of the period of limited authorization, the information system must be either authorized to operate or the authorization for further operation will be denied. Renewals or extensions to this interim authorization to operate will be granted only under the most extenuating of circumstances. This office will monitor the plan of action and milestones submitted with the accreditation package during the period of limited authorization.

A copy of this letter with all supporting security certification and accreditation documentation should be retained in accordance with the agency's record retention schedule.

Name,
Title

Date

Enclosure